(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 December 2004 (29.12.2004)

PCT

(10) International Publication Number
WO 2004/114045 A3

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/IB2004/001926

(22) International Filing Date: 10 June 2004 (10.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/606,659 25 June 2003 (25.06.2003) US

(71) Applicant *(for all designated States except US)*: **NOKIA INC.** [US/US]; 6000 Connection Drive, Irving, TX 75039 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WANG, Bing** [CN/US]; 5752 Lilac Blossom Ln., San Jose, CA 95124 (US). **CARD, James** [US/US]; 46 McKenna Drive, Nashua, NH 03062 (US). **SMITH, Gregory, J.** [US/US]; 3576 Sunnydays Lane, Santa Clara, CA 95051 (US). **SCOTT, Robert, Paxton** [US/US]; 655 South Fair Oaks Avenue, # H-104, Sunnyvale, CA 94086 (US).

(74) Agents: **BRANCH, John, W.** et al.; Darby & Darby P.C., P.O. Box 5257, New York, NY 10150-5257 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
29 November 2007

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: TWO-PHASE HASH VALUE MATCHING TECHNIQUE IN MESSAGE PROTECTION SYSTEMS

(57) Abstract: The invention provides a two-phase hash value matching technique in message protection systems. This invention further improves the performance of message protection systems by avoiding computations associated with sophisticated signature hash value (SSHV) where possible. A message protection system that implements the two-phase hash value matching technique caches rough outline hash values (ROHVs) of previously scanned objects. The system can roughly distinguish one object from another using ROHVs. The system performs an initial check using ROHVs before performing the relatively time-consuming computations associated with SSHVs.

WO 2004/114045 A3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/IB04/01926

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00

US CL : 713/168

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/168, 159, 172, 156, 176

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
two phase authentication, two phase hash, MAC, NMAC, UMAC, PMAC.

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST, GOOGLE, NPL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BELLARE et al. Keying Hash Functions for Message Authentication January 1996, pages 2, 8-9, 13-15	27-29

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
05 February 2005 (05.02.2005)	25 SEP 2007
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No.	Authorized officer Gregory Morse Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB04/01926

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Please See Continuation Sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.: 27-29

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB04/01926

BOX III. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING

I. Claims 1-11, drawn to a method of scanning objects and their particular value fields, such as a virus scanner scanning data structures, or reading data fields from an object like "inspectors".

II. Claims 12-26, drawn to an apparatus containing a particular data structure with two fields.

III. Claims 27-29, drawn to an apparatus of checking object consistency through hashes.

The inventions listed as Groups I-III do not relate to a single inventive concept under PCT rule "13.1" because, under PCT rule "13.2", they lack the same corresponding special technical features for the following reasons:

All the groups are directed towards reading and checking data from a particular data structure with a plurality of fields, but each group has special technical "features." Group I has a special technical feature directed to reading particular data fields of an object/class data structure passing through a device similar to "Inspectors" as seen in Object Oriented Programming, not required for Groups "II-III." Group II has a special technical feature directed to the actual data structure itself and how the data is organized, not required for Groups I, "III." Group III has a special technical feature directed to the scanning for the consistency of the object itself through a hashing technique not required for Groups "I-II." In contrast to Group I, Group III scans through a hash, and so consequently, the data that is read checks for the consistency of the object overall such as in "checksums." Unlike a mere reading of the fields within an object, the data derived from a hash cannot be recovered to acquire the original data it was drawn "from."